

I Claim:

1 1. A system for receiving and transmitting secure data on a server
2 computer using a shared key, comprising:
3 an encrypt/decrypt engine for encrypting and decrypting data
4 using the shared key;
5 a database of user shared keys for encrypting and decrypting
6 data for a specific user.

1 2. The system of claim 1, further including a secure data database
2 for storing encrypted data, and a private server key for encrypting and
3 decrypting data stored on the server.

1 3. The system of claim 1, wherein the encrypt/decrypt engine uses
2 a symmetric key encryption/decryption algorithm for encrypting and
3 decrypting data.

1 4. The system of claim 1, further including a web server engine
2 programmed to allow a user to send data securely using the
3 encrypt/decrypt engine.

1 5. The system of claim 1, further including a web server engine
2 programmed to allow a user to receive secure data using the
3 encrypt/decrypt engine.

1 6. A method for receiving secure data on a server computer using a
2 shared key, comprising the steps of:
3 receiving data on the server computer from a user, wherein the
4 data is encrypted with a user's key shared between the user and the
5 server computer;
6 decrypting the data with the user's key into decrypted data; and
7 processing the decrypted data.

1 7. The method of claim 6, wherein processing the decrypted data
2 includes the steps of:
3 encrypting the decrypted data with a private server key; and
4 storing the encrypted data in a database.

1 8. The method of claim 7, wherein processing the decrypted data
2 further includes the steps of:
3 decrypting the encrypted data with the private server key;
4 encrypting the data with a second user's key shared between
5 the second user and the server computer; and
6 sending the encrypted data to the second user.

1 9. The method of claim 8, wherein the encrypted data send to the
2 second user can only be viewed on a computer screen by the second
3 user.

1 10. The method of claim 6, wherein processing the decrypted data
2 further includes the steps of:

3 processing the data according to the user's instructions into
4 processed data;
5 encrypting the processed data using the user's shared key; and
6 sending the encrypted processed data to the user.

1 11. A computer-readable medium comprising program instructions
2 for receiving secure data on a server computer using a shared key,
3 comprising the steps of:

4 receiving data on the server computer from a user, wherein the
5 data is encrypted with a user's key shared between the user and the
6 server computer;
7 decrypting the data with the user's key into decrypted data; and
8 processing the decrypted data.

1 12. The computer-readable medium of claim 11, wherein processing
2 the decrypted data includes the steps of:
3 encrypting the decrypted data with a private server key; and
4 storing the encrypted data in a database.

1 13. The computer-readable medium of claim 12, wherein processing
2 the decrypted data further includes the steps of:
3 decrypting the encrypted data with the private server key;
4 encrypting the data with a second user's key shared between
5 the second user and the server computer; and
6 sending the encrypted data to the second user.

1 14. The computer-readable medium of claim 11, wherein processing
2 the decrypted data further includes the steps of:
3 processing the data according to the user's instructions into
4 processed data;
5 encrypting the processed data using the user's shared key; and
6 sending the encrypted processed data to the user.